VOLUME 17 ISSUE 3

KCJIS NEWS

NOVEMBER 2015

USER ACCOUNT REVIEW AND ACCESS CONTROL
KIP BALLINGER, IT SECURITY AUDITOR/TRAINER KHP

While conducting KCJIS security audits, it is not uncommon to find user accounts that have not been disabled after an employee leaves employment. In addition, it has been found that some user accounts are inadvertently given full administrative privileges when they were created. Attackers can exploit user accounts which are still valid in the system, but are no longer current. Discovering an obsolete yet still active account with full admin rights is a free pass around the information system. KCJIS Security Policies exist to mitigate these risks.

KCJIS Security Policy 5.5.1 (Account Management) requires that each agency manage their own information system accounts. This includes establishing, activating, modifying, reviewing, disabling, and removing accounts. The agency also must validate information system accounts at least once a year and document the validation process.

The annual review is the minimum policy requirement. As a best practice, it is recommended that user accounts be reviewed more frequently than the annual minimum requirement in order to mitigate the risk information system being exploited through one of these accounts. The risk of an attacker availing themselves through an obsolete, yet active, account increases with each day they are allowed to exist without being disabled.

INSIDE THIS ISSUE

Individual user accounts are typically found in KACIS, OpenFox, local applications such as CAD/RMS, and local networks (Active Directory). When a person is no longer employed by an agency, it is very important that their accounts are disabled in each and every one of these programs in a timely manner.

In order to ensure that obsolete accounts do not “slip through the cracks” and remain active, KCJIS Security Policy requires that the agency responsible for account creation be notified when: a user’s information system usage or need-to-know or need-to-share changes; when a user is terminated or transferred; or when associated accounts are removed, disabled, or otherwise secured. It is recommended, as a best practice, that information systems are configured to automatically disable any account which has been inactive for a specified period of time, e.g. 30 days.

When reviewing accounts, it is not only important to disable obsolete accounts, but also to review each active account. Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. Each agency must identify authorized users of the information system and specify their access rights and privileges. Granting access to the information system must be based on a valid need-to-know/need-to-share basis which is determined by assigned official duties and only to the satisfaction of all personnel security criteria.

As mentioned above, attackers love to discover and exploit obsolete, yet active, user accounts. They also love accounts with administrative rights. Organizational members with elevated privileges/rights are often targets of social engineering/spearfishing attacks as their accounts have higher permission levels and fewer restrictions on navigating through and accessing components (servers, etc.) in the information system.

USER ACCOUNT REVIEW AND ACCESS CONTROL– CONTINUED
KIP BALLINGER, IT SECURITY AUDITOR/TRAINER KHP

KCJIS Security Policy Section 5.5.2 (Access Enforcement) requires the information system to enforce assigned authorizations for controlling access to the system as well as any contained information therein. The information system controls must restrict access to privileged functions and security-relevant information to explicitly authorized personnel.

Access control policies and associated access enforcement mechanisms must be utilized by agencies to control access between users and objects such as devices, files, records, processes, programs, and domains in the information system.

It has also been discovered that some users had been given full administrative privileges when they were created. This typically happens when an account gets assigned to the Admin group rather than the Users group. KCJIS Security Policy Section 5.5.2.1 *(Least Privilege) requires each agency to enforce the most restrictive set of rights/privileges or access needed by users for the performance of specified tasks.* Each agency must implement least privilege practice based on specific duties, operations, or information systems as necessary in order to mitigate risk to Criminal Justice Information (CJI). This restricts CJI users' access to only authorized personnel with the need and right to know.

As job roles shift due to promotions, transfers, reassignments, etc. the performance of specified tasks may change as a result of being given different access privileges. Modifications to individual access privileges must be authorized and logs of access privilege changes must be maintained for a minimum of one year or at least equal to the agency's record retention policy- whichever is greater. All physical and logical access restrictions associated with these changes to the information system must be enforced.

Access control provides planning and implementation of mechanisms that restrict reading, writing, processing, and transmission of CJIS information as well as the modification of information systems, applications, services, and communication configurations allowing access to CJIS information.

In summary, regular reviews of agency user accounts and associated permissions (especially those with administrative privileges) will help mitigate risk to the information systems and any data they contain. Please refer to KCJIS Security Policy Area 5.5 for specific policy requirements in the areas of User Account Review and Access Control. Additional best practices and recommendations for access control policy and procedures can be found in NIST Special Publication 800-53 (Rev. 4)-C-1: Access Control Policy and Procedures; AC-2: Account Management; and AC-3: Access Enforcement.

DNA DATABANK
JOHN GAUNTT, PUBLIC SERVICE ADMINISTRATOR KBI

After eight years and over one hundred thousand samples, the DNA Databank has started to implement a new collection kit. This new kit is different; therefore, information about the kit is being provided to help everyone get started. If any agency has not received kits yet or when current supply run low, please get in touch with the Databank contacts:

Marilyn Timberlake	785-296-5461	marilyn.timberlake@kbi.state.ks.us
Jessica Watts	785-296-5083	jessica.watts@kbi.state.ks.us

To help every agency through this change, a training document about the new kit has been placed on the KCJIS Information tab. Scroll down to "**Lab**" to find three items of interest:

1. The procedure for collecting a DNA sample with the new kit: the EasiCollect.
2. Prelog procedures
3. DNA Databank training fall 2015 on PDF

These articles are up-to-date and provide more information. Feel free to contact either Marilyn or Jessica as well.

This is the last opportunity I will have the honor to write an article for the Databank. Effective September 28, 2015, I moved over to the Offender Registration Unit. Remember: the DNA Databank is a very effective tool for law enforcement; and we need every qualifying DNA sample to make it work!

UNICORNS AND OTHER MYTHS ABOUT CJIS COMPLIANCE
DON CATHEY, KCJIS INFORMATION SECURITY OFFICER

Remember those children's stories about unicorns, Hercules, and Atlantis? Perhaps one's parents used these stories to invoke a certain feeling, convey a specific concept, or encourage a desired behavior. These types of stories are called myths: "*a person or thing having only an imaginary or unverifiable existence,*" http://www.merriam-webster.com/dictionary/myth. They are not real. They don't exist.

Here are examples of modern day CJIS (Criminal Justice Information System) myths: "Our product is CJIS Certified!" "Our product is CJIS Approved!" "Our people are all CJIS authorized." "Our experts can guarantee your agency's CJIS compliance (for a small fee)." "We use government level Department of Defense approved encryption algorithms so your data is safe and compliant."

Unless the product being discussed is specifically a fingerprint scanner (the Federal Bureau of Investigation (FBI) CJIS only "certifies" the technical specification -resolution- of fingerprint scanners to be compatible with the Next Generation Identification system, formerly Integrated Automated Fingerprint Identification System (IAFIS)), then all of these stories and statements are mythical. There is NO such thing as "CJIS Certification," "CJIS Approval;" "CJIS Authorized," or any other credential currently offered by the FBI or any other entity that will ensure CJIS compliance.

This misconception typically occurs when vendors try to convince agencies that their products or services are capable of being "CJIS compliant." However, *each AGENCY and their implementation of products and services* are evaluated during triennial audits conducted by the Kansas Highway Patrol CJIS unit in order to determine their compliance with all FBI and Kansas Criminal Justice Information System (KCJIS) policies.

The policies are not simply written to a series of specifications that apply the exact same requirements for every agency, product, or circumstance. As explained in the Executive Summary, Introduction, and Section 2, these policies allow for each state and local agency to bolster the security policy to fit their own needs while attempting to avoid detailed rules about exact technologies. Instead, it tries to convey basic concepts that are applicable to many technologies and even for the different ways to implement them. For instance: encryption of Criminal Justice Information (CJI) is required outside a physically secure location. This policy does not mandate a specific encryption product or method: only that it must be certified by the National Institute of Standards and Technology (NIST) in order to meet the Federal Information Processing Standard (FIPS) 140-2 standard. NIST certification indicates a passing rating after proper testing of the *Implementation* of the encryption.

"The local agency may complement the CJIS Security Policy with a local policy, or the agency may develop their own stand-alone security policy;"
-FBI CJIS Security Policy 1.3

"The architectural independence of the Policy provides agencies with the flexibility for tuning their information security infrastructure and policies to reflect their own environments."
-FBI CJIS Security Policy 2.2

Consider policy 5.12.1.2 Personnel Screening for Contractors and Vendors that states: "in addition to meeting the requirements in paragraph 5.12.1.1, contractors and vendors shall meet the following requirements:

1. *Prior to granting access to CJI, __the CGA (Contracting Government Agency) on whose behalf the Contractor is retained shall__ verify identification via a state of residency and national fingerprint-based record check."*

This language says that each agency is responsible for ensuring that record checks are completed on personnel allowed to access CJI. Current policy states that a record check performed in another state does not grant compliance in Kansas. It is known that the FBI allows some flexibility *within each state*, but not from interstate record checks.

These policies are reviewed annually to keep them as current as possible. The FBI Information Security Officer (ISO) program office has resources available to show how to map the security policy for some newer technology trends. The Kansas Highway Patrol (KHP) CJIS Unit may provide assistance as well.

UNICORNS AND OTHER MYTHS ABOUT CJIS COMPLIANCE-CONTINUED
DON CATHEY, KCJIS INFORMATION SECURITY OFFICER KHP

Bottom line:

- Do not accept any vendor's claim of CJIS compliance.
- Every agency must verify that products or services are implemented in a way that will be compliant.
- Every agency must verify that all personnel with access to unencrypted CJI or systems used for CJI has been properly record checked in Kansas.

Contact your KHP information technology security auditor for more information.

IT'S ALIVE!
LESLIE MOORE, ISD DIRECTOR KBI

Kansas Bureau of Investigation is very proud to announce that the Leavenworth County District Attorney's Office and Wichita Municipal Court went live by connecting to the electronic disposition interface in September, 2015.

The interface connection allows agencies to submit dispositions directly from their records management software. This means that they do not have to provide additional data entry on the electronic form on the KCJIS (Kansas Criminal Justice Information System) web portal, and they will not have to use paper forms. This will ultimately save valuable time that can be utilized elsewhere.

Once these dispositions are transmitted, they will go directly into the appropriate criminal history record by matching the arrest transaction number, name, and date of birth of the defendant. Dispositions will be made available on the rap sheet almost instantaneously. If a disposition does not match a record, then it will be stored in a queue for further research and processing by the KBI Criminal History Records staff.

If any agency or vendor is interested in connecting to the electronic disposition interface, please contact Kristi Carter at Kristi.Carter@kbi.state.ks.us for more information.

FAILURE TO APPEAR CHARGES AND MUNICIPAL COURTS
KRISTI CARTER, RECORDS UNIT MANAGER KBI

It has come to the attention of Kansas Bureau of Investigation (KBI) that there is some confusion for Municipal Courts regarding the reporting of Failure to Appear (FTA) charges to the KBI Criminal History Records Unit. K.S.A 21-5915 defines FTA as a class B Misdemeanor; however, the statute specifically excludes failing to appear in Municipal Courts. There is no equivalent statute to charge an individual with FTA at the municipal level. Therefore, Municipal Courts should treat FTA as an administrative action to initiate a bench warrant for the original charge(s).

Instead of reporting an arrest for an FTA, the arresting agency should submit a second arrest for the original charge(s) with a new transaction number. The final court disposition should be reported on the transaction number for the first (original) arrest followed by the submission of a declination for the second arrest on the new transaction number.

If you have any questions please contact the KBI Records Unit at 785-296-2454.

THE NEW AGE OF EVIDENCE SUBMISSIONS: PRELOG

STEVE SISCO, FORENSIC SCIENTIST KBI

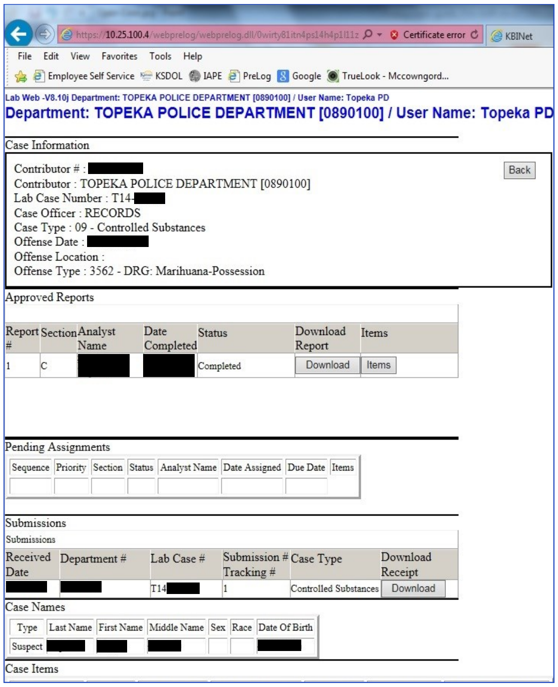
The Kansas Bureau of Investigation (KBI) Forensic Science Laboratories utilize Porter Lee's BEAST Laboratory Information Management System in order to maintain the chain of custody for evidence submitted to the laboratories for scientific analysis. Earlier this year, Lee's web browser based Prelog module program was activated to help streamline the evidence submission process for law enforcement customers. The Prelog module allows customers to Prelog evidence prior to submission to the laboratories. It also gives visual access to submitted evidence and available laboratory reports. This module is solely to be used by law enforcement customers of the KBI Forensic Science Laboratories.

To gain access to the Prelog module, law enforcement agencies must complete a PRELOG System Access Application (available on the KBI website http://www.kansas.gov/kbi/info/info_forms.shtml). Once the form has been completed, submit the form to the LIMS Administrator (LIMSAdmin@kbi.state.ks.us) for processing. When access is granted, users can log into Prelog through the KCJIS Portal, https://www.kcjis.state.ks.us. After logging in, click on the Prelog link on the left hand menu.

Prelogging Evidence: To start "prelogging" evidence, select the "**Evidence Prelog**" button, then the "**New Case**" button, and finally populate the following information tabs: **Case Info, Names, Items, and Lab Submissions**. This information is ***CRITICAL*** for ensuring the accuracy of the reports generated by the laboratories. When all the information is entered, Prelog will prompt a Prelog Packing Slip print out. After printing out a copy, transport the printed packing slip and corresponding evidence to the nearest KBI Forensic Laboratory for submission.

Case Inquiry: The Prelog module grants law enforcement agencies access to specific information regarding evidence status after being submitted to the KBI Forensic Science Laboratories for analysis.

In the "**Case Inquiry**" button, agencies can review case submissions and download/print copies of Submission Receipts shortly after evidence submission. Reports are available for download/printing through Prelog once the reports have been completed and released by the laboratory section. Submission receipts and laboratory reports are available in PDF format for ease of printing or incorporation into information management systems.



Lab Web -V8.10j Department: TOPEKA POLICE DEPARTMENT [0890100] / User Name: Topeka PD

Department: TOPEKA POLICE DEPARTMENT [0890100] / User Name: Topeka PD

Case Information

Contributor # : [redacted]
Contributor : TOPEKA POLICE DEPARTMENT [0890100]
Lab Case Number : T14-[redacted]
Case Officer : RECORDS
Case Type : 09 - Controlled Substances
Offense Date : [redacted]
Offense Location :
Offense Type : 3562 - DRG: Marihuana-Possession

Back

Approved Reports

Report #	Section	Analyst Name	Date Completed	Status	Download Report	Items
1	C	[redacted]	[redacted]	Completed	Download	Items

Pending Assignments

Sequence	Priority	Section	Status	Analyst Name	Date Assigned	Due Date	Items

Submissions

Submissions

Received Date	Department #	Lab Case #	Submission # Tracking #	Case Type	Download Receipt
[redacted]	[redacted]	T14[redacted]	1	Controlled Substances	Download

Case Names

Type	Last Name	First Name	Middle Name	Sex	Race	Date Of Birth
Suspect	[redacted]	[redacted]	[redacted]			[redacted]

Case Items

The KBI Forensic Laboratories Prelog initiative is continuing their commitment to provide timely forensic science services for the Kansas criminal justice system. The Prelog module helps reduce evidence submission times by giving contributors the ability to visually track evidence submitted for evidence as well as evidence receipts and laboratory reports submitted to the forensic laboratories.

For more information, a Prelog User's Guide is available for download on the KBI website: http://www.kansas.gov/kbi/info/info_forms.shtml. An instructional video offering additional assistance in starting the Prelog process is located both on the secured KCJIS website and KBI's public website: http://www.kansas.gov/kbi/info/info_forms.shtml under the **KBI Forms section**. The video is .mp4 formatted and is compatible with most video players (Windows Media Player, VLC Player, etc.). Due to file size, please download the file prior to viewing. NOTE: the video located on the KCJIS website will not play in Windows Media Player due to streaming limitations on the proxy server. KCJIS users will need to right click on the file, select "Save Target As," and save the file to view. For any additional information regarding the Prelog program, please contact one's servicing KBI Forensic Laboratory.

COME TO THE KSORT SIDE
JENNIFER SLAGLE, PROGRAM CONSULTANT KBI

In this day and age of rushing around to hurry up and get things done; everyone wants to make things easier for themselves. KsORT (Kansas Offender Registration Tool) can help do that!

By using KsORT, agencies would have access to historically reported information such as addresses and employment and information on restricted offenders (e.g. juveniles). Additionally, there will be access to advanced search options including vehicles, scars, and tattoos. Agencies can upload and store documents into KsORT for other agencies to access as well. KsORT is about working together to monitor registered offenders. Plus, KsORT is free!

If an agency is not ready to jump onto the KsORT bandwagon quite yet, they can still obtain read-only access. Any law enforcement agency (police department, sheriff's office, etc.), can benefit by "reading" the information on registered offenders. Read-only agencies would not be able to edit or modify any information.

The KsORT information database provides access to: **Offender, Alias, Alternate Identifiers, Scars/Marks, Tattoos, Licenses, Vehicle Information, Boat Information, Addresses, NIC, Employment, School Information, Internet Identifiers, Offenses, Images, Documents, Contact, and Verification.**

Here is what needs to done to obtain full access:

- Talk to the local Sheriff or Chief of Police and get him/her on board.
- The Commanding Officer will then contact Jennifer Slagle, Offender Registration Unit, to fill out a Memorandum of Agreement.
- If an agency is going to have full access to KsORT, then all users must attend training. Agencies with read-only access do not require training.
- All KsORT users must have a RSA SecureID token which can be obtained through a Terminal Agency Coordinator (TAC).
- Computers must have 3.25 GHz with 4G of memory, Internet Explorer 9 or later, and Adobe Reader for PDF viewing.
- And voila.....an agency is now able to use KsORT!

If an agency is interested in becoming a KsORT user or would like additional training on KsORT, please contact Jennifer Slagle by email at Jennifer.Slagle@kbi.state.ks.us or at 785-296-0945.

Criminal Justice Kansas Information System

The KCJIS Newsletter is published by the
Kansas Criminal Justice Coordinating Council

Derek Schmidt
Attorney General
Chair

Sam Brownback
Governor
Vice-Chair

Council Members

Kirk Thompson
Director
Kansas Bureau of Investigation

Justice Caleb Stegall
Chief Justice Designee

Ray Roberts
Secretary
Kansas Department of Corrections

Mark Bruce
Superintendent
Kansas Highway Patrol

Tim Keck
Governor Designee

Lee Davidson
Attorney
General Designee

KANSAS BUREAU OF INVESTIGATION

Alicia Madison
Newsletter Editor
1620 SW Tyler
Topeka, KS 66612
785-296-3302
Alicia.Madison@kbi.state.ks.us